DE UN MUNDO FÍSICO A UN MUNDO VIRTUAL, CRÍMENES CIBERNÉTICOS Y EL DERECHO PENAL EN PUERTO RICO

ARTÍCULO

*Elier A. Cardona Aquino**

I. Introducción

A. Sociedad

En el planeta habitan más de 7 mil millones[1] de seres humanos de diferentes abstracciones sociales, étnicas, económicas, educativas y religiosas. Esta diversidad de personas viven en grupos comunitarios que conforman lo que conocemos como sociedades.[2] Cada sociedad posee sus propias peculiaridades y necesidades que las diferencian una de las otras. Es prudente preguntarse ¿cómo estas sociedades compuestas de individuos de abstracciones heterogéneas pueden convivir en una comunidad de orden social?

Uno de los vehículos del orden social son las normas pautadas por la propia comunidad donde estos individuos habitan. A diferencia de las normas sociales[3]

---

* Estudiante de segundo año de la Facultad de Derecho de la Universidad Interamericana de Puerto Rico y poseedor de un bachillerato de Ingeniería en Computadoras. El autor desea agradecer al Prof. Fredrick Vega Lozada, LLM por la confianza depositada en este servidor y el honor de haber colaborado como su asistente de cátedra en su curso de Derecho Cibernético. Un agradecimiento especial para mi esposa Arleen, gracias por toda la motivación y apoyo en estos años.

[1] United States Census Bureau, *World Population Clock*, http://www.census.gov/population/popclockworld.html (accedido el 28 de abril de 2012).

[2] Real Academia Española, *Diccionario De La Lengua Española - Vigésima segunda edición*, http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=sociedad (accedido el 28 de abril de 2012).

[3] Ángel Latorre, *Introducción al Derecho*, 24 (3da ed., Ediciones Ariel 1971).

que pueden ser un tanto variantes de una sociedad a otra y aún dentro de una misma sociedad, la ley es la guía más clara para regular la conducta no deseada de un lugar.

Las leyes crean el marco de referencia de cómo deben conducirse las personas para mantener un orden social[4] y poder vivir en comunidad de forma armoniosa y ordenada.

B. Puerto Rico

Al igual que los ciudadanos de otros lugares en el mundo, los puertorriqueños no son ajenos a los males sociales.[5] Por tanto, al igual que en otros países, existen leyes que castigan las conductas que dan origen o perpetúan males sociales.[6] Queda claro que el ordenamiento jurídico penal puertorriqueño desde su origen fue pensado y creado para atender las conductas no deseadas del mundo que se conocía hasta ese momento, el mundo físico.

En las pasadas décadas Puerto Rico ha experimentado muchos cambios sociales. Uno de los grandes propulsores de este cambio social ha sido el acceso a tecnologías de comunicación tales como teléfonos móviles, computadoras y acceso al internet. Este acceso a la convergencia de tecnologías y la disponibilidad de estos equipos de comunicación no han sido por si solos el motor de cambio, el bajo costo, subsidios gubernamentales y otros tipos de incentivos de mercadeo han permitido que las personas independientemente de su nivel social y económico sean poseedores y usuarios de estas nuevas herramientas de comunicación.

C. Tecnología

Con el acaecimiento de la era tecnológica, la nueva sociedad puertorriqueña cada día abandona más y más los medios tradicionales de realizar sus quehaceres cotidianos. En vez de personarse en las diferentes dependencias del gobierno para realizar los pagos de las facturas de las utilidades o caminar a un centro comercial para adquirir bienes o servicios, incluso enviar una postal a un ser querido, ahora los puertorriqueños se han insertado al nuevo mundo tecnológico utilizando el internet para realizar todas estas tareas y para estar más cerca de sus seres queridos. ¿Cuál es la motivación de los puertorriqueños para esta transición?

El internet les permite a las personas poder estudiar y trabajar a distancia, hacer transacciones bancarias sin tener que ir a una institución financiera, hacer video conferencias con potenciales clientes o seres queridos. En resumen podemos

---

[4] Ángel Latorre, *Introducción al Derecho*, 50 (3da ed., Ediciones Ariel 1971).

[5] Puerto Rico Daily Sun, *No end in sight to criminal fatalities,* http://www.prdailysun.com/?page=news.article&id=1315224674, (accedido el 2 de abril de 2012).

[6] Exposición de Motivos, Código Penal, Ley Núm. 149 de 18 de junio de 2004.

afirmar que el internet permite realizar actividades cotidianas de forma rápida, costo efectiva y con la mayor comodidad. Sin duda estas tres virtudes del internet son altamente valoradas en nuestra sociedad.

El internet trasciende de su origen cerrado y de carácter militar a una etapa libre y abierta propulsada en su inicio por la academia y ahora por los movimientos sociales. La misma naturaleza libre y abierta del internet que no conoce fronteras geográficas o jurisdicciones territoriales crea conflictos al momento de encausar individuos que se le imputan cometer delitos por medio de estas redes de comunicación. No existe un tratado o ley de aplicación global para dilucidar las controversias que surgen del mal uso de las redes de comunicación. El internet es global, pero las controversias que genera su mal uso crean problemas que retan las fronteras geográficas y las leyes de todos los países que están conectados a él. A falta de una regulación uniforme o global, queda en cada Estado regular el mal uso[7] que se le da a este instrumento que se ha convertido en herramienta indispensable en el diario vivir de las personas y en la economía mundial.[8]

D. Crímenes a través del internet

El principio de legalidad de nuestro actual Código Penal esboza que "*No se instará acción penal contra persona alguna por hechos que no esté expresamente definido como delito en este Código o mediante ley especial, ni se impondrá pena o medida de seguridad que la ley no establezca con anterioridad a los hechos.*"[9] Tampoco se podrá crear ni imponer delitos, penas, ni medidas de seguridad por analogía[10] a una conducta que se parezca más no sea igual a la tipificada en el Código Penal. Por tanto los delitos tipificados del mundo físico no serán de aplicación a las transgresiones realizadas en el internet o mundo virtual a menos que surja de su texto que sí aplicarán. De forma limitada existen delitos tipificados en nuestro Código Penal y leyes especiales relacionadas a crímenes cibernéticos. Aun así, existen tres retos fundamentales al momento de encausar a personas por estos delitos cometidos a través de las redes cibernéticas. Veremos cómo se analiza y diferencian la identificación del sujeto, la jurisdicción y el manejo de evidencia digital en el mundo virtual vis a vis el mundo físico.

---

[7] Puerto Rico Daily Sun, *Cybercrimes a growing threat in Puerto Rico*, http://www.prdailysun.com/news/Cybercrimes-a-growing-threat-in-Puerto-Rico (accedido el 2 de abril de 2012).

[8] Forbes, *G-20 Internet Economy To Reach $4.2 Trillion In 2016*, http://www.forbes.com/sites/ericsavitz/2012/01/27/g-20-internet-economy-to-reach-4-2-trillion-in-2016 (accedido el 2 de abril de 2012).

[9] Ley Núm. 149- 2004 2004 L.P.R.§33, Art. 2.

[10] Ley Núm. 149- 2004 2004 L.P.R.§33, Art. 3.

II. Retos de los crímenes cibernéticos

A. Identificación

¿Cómo se identifica una persona que se le acusa de haber cometido un acto delictivo a través del internet?

Precisamente éste es uno de los problemas fundamentales a la hora de poder encausar a una persona por un delito cometido a través de las redes cibernéticas. En Puerto Rico si no se puede identificar al sujeto, no habrá encausamiento del mismo debido a que la identificación del imputado está revestida por las garantías contenidas en el debido proceso de ley[11] de la Constitución.[12]

En el mundo físico el problema de identificación es en muchas instancias complejo, pero existen varios mecanismos para logar la identificación de un imputado. La identificación podría realizarse a través de distintos métodos tales como: una rueda de detenidos, examen de voz, por fotografías; en el mundo virtual resulta más difícil ya que la víctima del delito no podrá identificar a su victimario utilizando métodos sensoriales. Entonces, ¿cómo se identifica a un sospechoso de cometer un delito en el internet?

El contestar esa pregunta requiere una explicación de los conceptos *estar* o *navegar* en el internet. La mejor forma de explicar este proceso es empleando una analogía entre acceder el internet y ver televisión por servicio de cable tv (CATV). Como es conocido, para ver televisión por servicio de cable tv es requerido como mínimo un televisor para ver la programación disponible, una caja convertidora provista por la compañía del CATV para decodificar la señal digital que envía dicha compañía, en imágenes que se puedan ver en el televisor; además es necesario el servicio de canales del proveedor de televisión por cable.

En esencia, como mínimo se requieren tres cosas para navegar el internet. Primero se necesita una computadora, una tablet o un teléfono móvil que servirá de interface o pantalla para que el usuario pueda ver las páginas de internet. En segundo lugar esa computadora, tablet o teléfono móvil requiere un dispositivo de conexión de redes alámbrico o inalámbrico que permita recibir y transmitir data al proveedor de servicio de internet[13] (ISP). El ISP ofrece los medios tecnológicos de redes de comunicación para que podamos navegar en el internet. Ya sea gratuito o pagando por el servicio, es necesario tener el servicio de un ISP para navegar el internet.

Explicado lo anterior, queda la pregunta planteada, ¿cómo se identifica a un sospechoso de cometer un delito en el internet?

---

[11] En el caso, *Pueblo v. Hernández González*, 2009 T.S.P.R. 7 se explica en detalle la doctrina del proceso de identificación y su relación al debido proceso del ley en Puerto Rico y Estados Unidos.

[12] Const. P.R. Art. II § 7; Const. EE.UU. Enmienda XIV.

[13] En adelante haremos referencia al proveedor de servicio de internet utilizando las siglas ISP por sus siglas en inglés.

Todas las computadoras al conectarse al internet dejan huellas digitales en las computadoras del ISP. Cuando un cibernauta se conecta al ISP por medio de una computadora, tablet o teléfono móvil, el ISP registra un número alfanumérico de identificación "único" del dispositivo de conexión de redes que se conoce como el "MAC address",[14] en adición le asigna una dirección de IP[15] a esa computadora, tablet o teléfono móvil en las bitácoras, mejor conocidos como "logs" del ISP junto a la fecha y hora de conexión.

Entonces, ¿por qué no identificar a una persona usando su dirección de IP?, el ISP tiene la hora y fecha de conexión y el "MAC address" del dispositivo inalámbrico de conexión, ¿no sería esto más que suficiente para identificar el dispositivo y el usuario que está haciendo uso del mismo? La respuesta es *NO*. Veamos la siguiente situación de hechos.

Héctor residente del Condominio Sol adquiere el servicio inalámbrico de internet de alta velocidad del ISP Puerto Rico Súper Internet. Él llega a su apartamento y conecta el dispositivo de conexión de redes inalámbricas (wireless router)[16] que le entregaron en Puerto Rico Súper Internet. Héctor está fascinado con la conexión súper rápida de su nuevo servicio y la conveniencia de poder usarlo por todo el apartamento sin estar conectado a un cable. El mismo día, Marcos residente del complejo aledaño al de Héctor, que no tiene servicio inalámbrico de internet se percata de la presencia del dispositivo de conexión de redes inalámbrica de Puerto Rico Súper Internet que le pertenece a Héctor. Marcos se conecta al dispositivo de conexión de redes inalámbricas de Héctor y comienza a hacer búsquedas y descargas de fotos de pornografía infantil y envía amenazas de muerte a niñas en un "chat room" que resultaron ser agentes encubiertos de la policía. El problema es que el ISP no distingue entre las páginas visitadas por Marcos de las visitadas por Héctor, para el ISP todas las páginas visitadas habrían sido originadas por el "wireless router" de Héctor.

Esta situación ejemplifica el por qué una dirección de IP no es lo mismo que una persona.[17] Claramente se desprende del ejemplo anterior un serio problema al momento de identificar a un sospechoso de cometer un delito cibernético. Un posible método de investigación para una situación de hechos como la antes presentada podría ser de la siguiente manera. Primero el Ministerio Público solicitaría la identificación del subscriptor del servicio de internet mediante una orden judicial al ISP utilizando la fecha y hora junto a la dirección de IP obtenida del "chat room".

---

[14] The Institute of Electrical and Electronics Engineers, *IEEE Standard for Local and Metropolitan Area Networks:Overview and Architecture*, http://standards.ieee.org/getieee802/download/802-2001.pdf, (accedido el 2 de abril de 2012).

[15] The Internet Engineering Task Force, *Internet Protocol - DARPA Internet Program Protocol Specification* (September 1981), http://tools.ietf.org/html/rfc791, (accedido el 2 de abril de 2012).

[16] Para esta situación de hechos el "wireless router" es el dispositivo que permitirá que varias computadoras de forma inalámbrica compartan la señal de internet que viene del ISP.

[17] *Internationale v. John Does 1-1017*, 2:11-cv-02068-HAB-DGB (CD. III, 2011).

Con esa información el ISP podrá hacer una correlación de la dirección de IP con el "MAC address" junto a la fecha y hora de la conexión. Hecho lo anterior, el "ISP" identificaría a qué cliente le pertenece ese "MAC address" y dirección de IP en esa fecha.

Ahora, con la información provista por el ISP, ¿a la puerta de quién tocarán los agentes de ley y orden cuando tengan en su poder una orden de registro y allanamiento? Tocarán a la puerta de Héctor ya que la dirección de IP y el "MAC address" registrados en el ISP son los que corresponden al equipo que le proveyó Puerto Rico Súper Internet, el "wireless router" que le dieron a Héctor. La computadora de Héctor y la de Marcos se conectaron inalámbricamente al "wireless router" y este equipo es el que se conecta al ISP. El ISP solo ve la conexión al "wireless router" y no una conexión independiente a la computadora de Héctor y otra conexión independiente a la computadora de Marcos. Para el ISP, Marcos no existe, toda la actividad cibernética proviene de la cuenta y del equipo Héctor.

Realizado el anterior registro y allanamiento de la computadora y demás equipos de comunicación y almacenaje de información digital, el Ministerio Público concluye que no existe evidencia digital que vincule a Héctor con el crimen cibernético bajo investigación. Ahora el Ministerio Público tendría que buscar otro sospechoso y para eso tendría que solicitar otra orden judicial para un requerimiento de información sobre todas las páginas de internet que se visitaron por el titular de la cuenta. Esto se logra identificando la dirección de IP y "MAC address" registrados en los sistemas del ISP. Ahora se tiene que correlacionar las páginas registradas en el ISP como visitadas ese día con las páginas frecuentadas por Héctor.

Digamos que Héctor tiene una sola cuenta de banco y la misma es del Banco de Puerto Rico y todos los días verifica su estado de cuenta por internet. A su vez, Marcos tiene una cuenta de banco en el Banco Socios Elite y también verifica con frecuencia su estado de cuenta por internet. Inspeccionando los "logs" suministrados por el ISP, el Ministerio Público observa las páginas de internet visitadas antes y después de las amenazas hechas en el "chat room". Haciendo ese ejercicio se percata que hay unas visitas al portal cibernético de miembros del Banco Socios Elite momentos antes de las visitas a las páginas de los chat rooms, banco del cual Héctor no es miembro. El Ministerio Publico mediando orden judicial debe hacer un requerimiento de información al Banco Socios Elite para verificar quien accesó a su cuenta de banco a la fecha y hora que arrojó el "log" del ISP. Una vez identificado el dueño de la cuenta, que en este caso se determinó que fue Marcos, se deberá hacer un registro y allanamiento de la computadora y equipos de comunicación de Marcos para corroborar si en efecto existe la evidencia digital para encausarlo.

La situación anterior presenta un problema evidente, si múltiples personas se conectan al mismo equipo que se conecta al ISP y luego el ISP no puede discernir entre los que estaban conectados, ¿cómo se sabe quién cometió el acto delictivo? Más interesante, digamos que fue el mismo Héctor el que incurrió en conducta delictiva, éste podría escudarse bajo el argumento de que fue otra persona que se

conectó a su servicio de internet de forma no autorizada y realizó los actos ilícitos.

Esta situación de hecho sólo toca la superficie de un gama de situaciones para la identificación de un sospechoso de cometer un crimen cibernético. Queda en evidencia cuan sencillo podría ser cometer delitos cibernéticos sin dejar un rastro digital con sólo utilizar el servicio de internet de otra persona. Existen situaciones en que sólo se podrá determinar mediante el examen de evidencia digital si en efecto el equipo bajo análisis forense fue el que se utilizó para cometer o no los actos delictivos pero no así quien realmente lo hizo.

B. Jurisdicción

Siendo el internet una red de computadoras global donde sus integrantes pueden estar en cualquier rincón del planeta, ¿cómo se podría tener jurisdicción sobre estas personas que están dentro y fuera de nuestro territorio por una conducta tipificada en nuestro Código Penal?

Nuestro Código Penal en su Artículo 6[18] establece que la ley penal de Puerto Rico será de aplicación a delitos consumados o intentados dentro de la extensión territorial de Puerto Rico. En el Artículo 7[19] del mismo Código nos aclara en su inciso (a) que habrá jurisdicción cuando: *"Cuando una parte de la conducta delictiva se lleva a cabo en la extensión territorial del Estado Libre Asociado de Puerto Rico."* y en el inciso (d) del mismo artículo nos dice que también habrá jurisdicción: *"Cuando según los tratados o convenios ratificados por los Estados Unidos de América, el delito puede ser procesado en el Estado Libre Asociado de Puerto Rico"*.

Tomemos la situación de hechos anterior entre Héctor y Marcos. Ahora modifiquemos la situación de hechos ubicando a Marcos en Hungría. Marcos en esta nueva situación de hechos cometió el delito de *alteración y uso de datos personales en archivos*[20] desde Hungría en contra de Héctor. Siendo Héctor ciudadano americano y residente en Puerto Rico, ¿podría el Ministerio Público de Puerto Rico tener jurisdicción para instar acción penal contra Marcos residente fuera del territorio?

Hagamos un escrutinio a la luz de los artículos 6 y 7 del Código Penal y los hechos presentados. El Artículo 6 requiere que el acto delictivo fuese consumado o intentado dentro de la extensión territorial de Puerto Rico, efectivamente Marcos consumó el acto en el territorio ya que Héctor se encontraba en Puerto Rico con su computadora. El Artículo 7 inciso (a), exige que una parte de la conducta delictiva se haya llevado a cabo en el Estado Libre Asociado, a la luz de los hechos antes presentados se puede percibir que el génesis de la conducta tipificada fue en

---

[18] Ley Núm. 149- 2004, 2004 L.P.R.§33, Art. 6.

[19] Ley Núm. 149- 2004, 2004 L.P.R.§33, Art. 7.

[20] Ley Núm. 149- 2004, 2004 L.P.R.§33, Art 183.

Hungría pero la conducta tipificada del delito cibernético fue en Puerto Rico.[21] Por último el Artículo 7 inciso (d) nos dice que Puerto Rico podría tener jurisdicción penal si existiese un tratado o convención ratificado por los Estados Unidos. Tanto Hungría como Estados Unidos son países signatarios de la Convención de Crímenes Cibernéticos.[22] Ambos países han ratificado dicha convención la cual ofrece mecanismos para la colaboración entre signatarios en los temas de delitos cibernéticos.

Estados Unidos es un país signatario con reservas en el cumplimiento de algunas de las disposiciones del convenio, un ejemplo de dichas reservas es en relación a la Sección 9 párrafo (2)(c) del convenio que exige legislación prohibiendo las imágenes realísticas de menores en actos sexuales. Esta disposición del convenio esta en contraposición a lo establecido jurisprudencialmente en el caso *Ashcroft v. Free Speech Coalition*[23] en el cual se estable que las imágenes realísticas de menores sexualmente explicitas están protegidas por la Primer Enmienda de la Constitución de la Constitución de los Estados Unidos. Finalmente, la situación presentada cumpliría con las exigencias del Artículo 7 inciso (d). No es necesario que se cumplan todos los requisitos del los Artículos 6 y 7, con cumplir uno de ellos sería suficiente para tener jurisdicción penal.

C. Evidencia digital

El Estado tiene una obligación de cumplir con el mandato constitucional del debido proceso de ley durante todo el proceso del encausamiento criminal de una persona imputada de acto delictivo. En el curso de una investigación criminal es de vital importancia que se preserve la integridad de los equipos electrónicos que tengan la capacidad de almacenar información[24] de forma digital. Siempre que las personas hacen uso de artefactos de comunicación dejan huellas de evidencia digital. Estas huellas de evidencia digital se almacenan en lugares como el disco duro de una computadora, la memoria USB que esta en un llavero o incluso la tarjeta SD de un cámara digital. Las huellas a su vez pueden ser tan variadas como fotos tomadas, archivos borrados, historial de navegación de internet entre otros. El poder recuperar esta información de forma oportuna es cada vez más importante dado la dependencia y el uso preferente de las personas de artefactos electrónicos con capacidad de almacenaje de datos digitales, entiéndase computadoras, teléfonos, "tablets", entre otros. Es relativamente fácil manipular la información contenida en estos dispositivos de almacenaje y búsqueda de datos. Por ende, es necesario que la

---

[21] Ley Núm. 149- 2004, 2004 L.P.R.§33, Art. 20.

[22] Council of Europe - Treaty Office, *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accedido el 2 de abril de 2012).

[23] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

[24] Ejemplo: Discos duros, DVD, CD, memorias externas.

extracción y el análisis de esta evidencia digital se realice por personas que posean un alto dominio tecnológico y conocimientos en los protocolos de manejo de los diferentes tipos equipos electrónicos encanutados.

En la actualidad El Instituto de Ciencias Forenses (ICF) es la entidad del Estado que lleva a cabo el análisis de la evidencia digital recopilada en el transcurso de una investigación criminal. La labor principal del laboratorio de criminalística del ICF es recuperar la evidencia digital evitando la modificación o alteración a las fechas de creación, modificación y último acceso de los archivos del equipo incautado.

III. Recomendaciones y conclusión

La problemática de crímenes cibernéticos no podrá ser propiamente atendida con leyes parchadas y sin cohesión dentro de un código penal. Los crímenes cibernéticos por su complejidad y características particulares deben tener leyes especiales o una sección propia dentro del Código Penal donde se recojan los delitos ordenados por tópico de conducta delictiva. Un ejemplo de un esfuerzo en esta dirección es el proyecto 2408 radicado por la Presidenta de la Cámara de Representantes, Jennifer González, titulado "Cyber Code of 2010"[25] el cual agrupa legislación de varios delitos cibernéticos comunes como el cyberbulling, distribución de pornografía infantil, entre otros. Aunque el mismo tuvo un informe negativo en el Senado, entendemos que es meritorio desarrollar nueva legislación conducente al primer Código Cibernético de Puerto Rico. Aún teniendo un Código Cibernético que fuese perfecto en derecho, éste no sería eficaz si no existe un cuerpo especializado de fiscales dentro del Departamento de Justicia dedicados exclusivamente a atender estos crímenes.

Sería ideal que este grupo de fiscales posean grados académicos en áreas tales como ingeniería de computadoras, sistemas de información, ciencias de computación o grados tecnológicos relacionados. Sin embargo, esto no significa que fiscales con preparación académica distinta a la recomendada puedan hacer efectivamente el trabajo, ciertamente podrían hacer el trabajo, pero esto requerirá que los fiscales sean adiestrados y capacitados en estas complejas disciplinas redundando así en una dilación de disponibilidad de personal hábil para trabajar estos casos de forma inmediata

Al momento de la redacción de este escrito, existe un esfuerzo encaminado por el Representante de la Cámara José Aponte en el proyecto 3896[26], para la creación de la Unidad Investigativa de Crímenes Cibernéticos (UICC) adscrita el Departamento de Justica, la cual estaría a cargo de investigar y procesar delitos y/o faltas graves y menos graves relacionadas con el derecho a la intimidad, propiedad,

---

[25] P. de la C. 2408, 16ta. Asamblea Legislativa, 3ma Session Ordinaria (24 de enero de 2010).

[26] P. de la C. 3896, 16ta. Asamblea Legislativa, 7ma Session Ordinaria (30 de marzo de 2012).

identidad y la seguridad en las transacciones comerciales, cuando se cometieren utilizando medios electrónicos, como el Internet y la computadora; y para otros fines relacionados. Esta medida legislativa es un paso esencial en la lucha contra los crímenes cibernéticos, pero por si sola se quedaría corta en su eficacia si carecemos de laboratorios en Puerto Rico para el análisis forense de la evidencia digital que se recopila en las investigaciones. Oportunamente, el Representante Aponte atiende esta situación en el proyecto 3906[27] de su autoría, el cual crearía el Laboratorio Tecnológico especializado en Crímenes Cibernéticos, adscrito al Departamento de Justicia. Este laboratorio tendría a su cargo recopilar, extraer, preservar y analizar la evidencia relacionada a crímenes cibernéticos.

Pensemos por un momento que contamos con todo lo antes recomendado, entiéndase una unidad especializada de delitos cibernéticos, fiscales especializados en la materia y un laboratorio de primer orden para hacer la labor forense. Los jueces necesitan también conocer sobre los temas y disciplinas tecnológicas, no a la misma capacidad de un profesional de dichas disciplinas, pero a un nivel que le permita tener los elementos de juicio básicos para aquilatar de forma lógica e inteligente la prueba que en su día le sea presentada. Esto podría lograse con la creación de salas especiales con jueces con grados académicos relacionados a la tecnología o altamente adiestrados en dichos temas. Estos adiestramientos podrían estar dentro de un currículo de estudio y capacitación el cual sea diseñado en una colaboración interdisciplinaria entre la academia, el sector privado y las agencias de ley y orden. El currículo podría estar a cargo de la Oficina de Administración de Tribunales para garantizar un mínimo de destrezas para los fiscales y jueces en las propuestas unidades y salas especializadas.

No podemos finalizar sin enfatizar cuan importante es la educación a la ciudadanía en la lucha contra los crímenes cibernéticos. El tema debe tener un interés apremiante cuando en Puerto Rico existen ciudadanos muy vulnerables a estos tipos de crímenes. A modo de ejemplo, en Puerto Rico existe una creciente población de niños a nivel elemental que poseen teléfonos inteligentes con capacidad de conectarse al internet, recibir e enviar mensajes de texto y correos electrónicos. Del mismo modo, existe una creciente población de la tercera edad que cada día más se insertan al uso del internet como vehículo para estar en contacto con sus seres queridos. Por sus características peculiares, estos grupos son altamente susceptibles y propensos a ser víctimas de delitos cibernéticos. El uso correcto de la tecnología y la concientización sobre los peligros que existen en el mundo cibernético es una función que debe asumir la familia, las instituciones educativas, la industria privada y el Estado.

En la mayoría de los casos, los crímenes del mundo cibernético no tienen rostro, pero las víctimas de estos crímenes están en el mundo físico que todos vivimos y sí tienen rostro y caminan entre nosotros todos los días.

---

[27] P. de la C. 3906, 16ta. Asamblea Legislativa, 7ma Session Ordinaria (17 de abril de 2012).

Puerto Rico no sólo está a tiempo para crear la legislación y el andamiaje educativo de avanzada necesarios para atender esta problemática antes de que se convierta en un problema social, si no que también cuenta con estudiantes de derecho, abogados y jueces prestos para aportar los conocimientos y talentos necesarios para el éxito de esta propuesta.